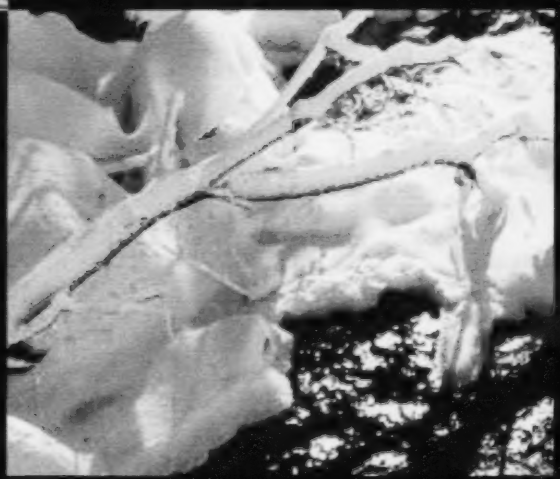
COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report



2011-2012

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984, Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: 613-992-3044
Fax: 613-992-4096
Website: www.ocsec-bcest.gc.ca

Cat. No. D95-2012
ISSN 1206 - 7490

Cover photos: Malak

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

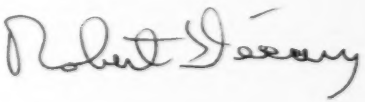
June 2012

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my annual report on my activities and findings for the period of April 1, 2011, to March 31, 2012, for your submission to Parliament.

Yours sincerely,



P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

BIOGRAPHY OF THE HONOURABLE ROBERT DÉCARY, Q.C.

The Honourable Robert Décary, Q.C., was appointed Commissioner of the Communications Security Establishment on June 18, 2010.

Commissioner Décary was born in Montréal in 1944. He received his education at Collège Jean-de-Brébeuf (BA), at Université de Montréal (LL.L.) and the University of London (LL.M.). He was called to the Québec Bar in 1967 and named Queen's Counsel in 1986.

In the course of a career dedicated to public office, the law and journalism, he was Special Assistant to the Honourable Mitchell Sharp (then Canada's Secretary of State for External Affairs) (1970–1973), Co-Director for Research on the Task Force on Canadian Unity, the Pepin-Robarts Commission (1978–1979) and member of the French Constitutional Drafting Committee of the Federal Department of Justice (1985–1990).

He practised law in Montréal, then in Gatineau, where, in the firm Noël, Décary, he specialized in representing many law offices and the Attorney General of Québec before the Supreme Court of Canada.

He has written a number of feature articles for *Le Devoir* and *La Presse*, and has contributed to many legal journals and textbooks. He is the author of *Aide-mémoire sur la Cour suprême du Canada* (1988) and of *Chère Élize* (or *The Long and the Short History of the Repatriation*) (1983).

He was a member of the Federal Court of Appeal from 1990 to 2009. In 2009, he was appointed arbitrator of the Court of Arbitration for Sport in Lausanne, and in 2010 he became a member of the Sport Dispute Resolution Centre of Canada.

COMMISSIONER'S MESSAGE

The primary purpose of this report is to inform the Minister of National Defence of my activities during the fiscal year ending March 31, 2012. I will make mention of the results of reviews I conducted into the operations of the Communications Security Establishment Canada (CSEC) during the past year, as well as review projects currently under way and those that I expect to undertake in the next few months. I will also refer to other activities that I and my office have conducted, especially those meant to keep us abreast of the latest developments in Canada and abroad in the area of review of security and intelligence agencies.

Two-thirds of the way through my three-year mandate, I am obliged to note that the public, and sometimes even so-called experts, continue, because of a lack of knowledge, to misjudge the respective roles of Canada's various intelligence agencies and, consequently, those of the various review bodies. There is a reason for this ignorance. The secret nature of the activities of intelligence organizations is such that any attempts at educating the public come up against a culture of silence that makes one keep quiet even about what is known or what could be made known. To paraphrase a well-worn expression, the fear that one might see certain trees is such that one is not allowed to describe the forest. In my opinion, it is possible, without going into details it would be inappropriate to divulge, to employ simpler and more comprehensible language and thus ensure that public debates are not held on false premises.

In my message of last year, I briefly described my own mandate and that of CSEC. This year, I shall be revisiting this in greater detail in my report.

Technology is developing at a staggering pace. CSEC's expertise in communications technology results in its providing assistance, pursuant to its mandate, to other members of Canada's security and intelligence community, particularly the Canadian Security Intelligence Service (CSIS). This year, as I pursue my efforts to inform the public through

this report, I would like to better define the respective roles of CSEC and CSIS. I find that these roles are frequently misunderstood.

When acting on its own initiative, CSEC does not have the right, under its enabling legislation, to target anyone within Canada or any Canadian outside Canada. However, CSEC also has a mandate to lend assistance to such organizations as CSIS, which might, upon request, lead to an involvement with a Canadian or someone on Canadian soil. In providing such assistance, CSEC is subject to the laws governing the organization that has made the request.

Since CSIS, under its enabling legislation, is concerned with threats to the security of Canada and may conduct its investigations using methods including the interception of private communications, the invasion of the privacy of Canadians is inherent in these activities, and Parliament wanted these activities to take place only upon the securing of a judicial warrant. Accordingly, when CSIS is executing such a warrant and requests the assistance of CSEC, CSEC is in effect simply taking part in an activity already authorized by a court. It would be superfluous to require another warrant at that point. My predecessors have reviewed the assistance provided to CSIS by CSEC. This year, I undertook an in-depth review, which I will complete in the next few months, of certain activities in which CSEC acts on a request of CSIS.

Furthermore, since CSEC is only authorized to target non-Canadians outside Canada, any interception of private communications involving Canadians is as unintentional as it is unforeseeable. Therefore, Parliament has required that these activities of CSEC that could unintentionally breach the privacy of Canadians be the object, not of a warrant, but of a ministerial authorization issued by the Minister of National Defence. This ministerial authorization, however, does not amount to a blank cheque; it comes with significant requirements, some legal and others that the Minister may prescribe, to ensure that, should the privacy of a Canadian become involved, measures are in place to protect it.

Increased cooperation between CSEC and CSIS in turn requires increased cooperation between the organizations that review them. This is not easily done, as the laws governing review bodies set up highly compartmented competencies that do not encourage pooling energies and resources. Lately, I have been working on finding ways of making the reviews that my office and the Security Intelligence Review Committee (SIRC) each undertake more complementary, to satisfy myself that no activities of CSEC and CSIS elude review. Paragraph 273.63(6) of the *National Defence Act* allows the Governor in Council to authorize me to engage in any related activity. Article 54 of the *Canadian Security Intelligence Service Act* allows the Minister of Public Safety and Emergency Preparedness to request from SIRC a "special report concerning any matter that relates to the performance of its duties and functions". I am of the opinion that my office and SIRC could, by virtue of these provisions, be asked to conduct a joint review or complementary reviews of certain activities involving both CSEC and CSIS. This approach would be squarely in keeping with the recommendations formulated by Justice Dennis O'Connor, in his second report of the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, on the system for reviewing security and intelligence organizations in Canada.

This annual report would not be complete if I did not highlight certain major changes in the top management of CSEC and in its status.

Last January, John Adams, who had been Chief of CSEC for six years, was appointed as Senior Advisor to the Privy Council Office and as Skelton-Clark Fellow to the Queen's University School of Policy Studies. I am in a position to testify just how much he was able to develop a culture of respect for privacy within CSEC. There will, of course, always be an inevitable and necessary climate of tension between a review body and the organization being reviewed. The challenge, then, for the heads of the two organizations is to make sure this tension is business-like and productive. To my mind, this has been the case.

John Forster, a seasoned senior civil servant, assumed leadership of the CSEC on January 30, 2012. I have met with him on several occasions and I already discern in him the traits of his predecessor. I am confident that our relationship will be marked by courtesy and respect. My team and I organized an intensive information session for the new Chief in order to present him with the clearest possible picture of how I carry out my review mandate under the Act.

Incidentally, until November 16, 2011, CSEC had been under guardianship of a sort, reporting both to the Deputy Minister of National Defence for its administration and finances and to the National Security Advisor to the Prime Minister for its operations and policies. On that day, CSEC became an autonomous body in the National Defence Minister's portfolio with departmental status. Its Chief acquired the rank of Deputy Head and reports directly to the Minister.

I do not expect this change of status to have any impact on the relationship between my office and CSEC. However, I am of the view that the requirement to report to the National Security Advisor to the Prime Minister allowed a broader government perspective on national security to be applied to CSEC operations and policies, and I will be watchful whether CSEC's new autonomy results in any weakening of its accountability and compliance control framework.

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

Overview

- My mandate (and CSEC's) is set out in Part V.1 of the *National Defence Act*.
- I operate at arms-length from government.
- I submit detailed classified reports of my reviews of CSEC to the Minister of National Defence.
- My recommendations aim to reduce risks of non-compliance with the law by CSEC and to strengthen its practices to protect the privacy of Canadians.

My mandate under the *National Defence Act* consists of three key functions:

1. **reviewing CSEC activities** to ensure they comply with the law;

2. **conducting investigations** I deem necessary in response to complaints about CSEC; and

3. **informing the Minister** of National Defence and the Attorney General of Canada of any CSEC activities that I believe may not be in compliance with the law.

Under the *Security of Information Act*, I also have a mandate to receive information from persons who are permanently bound to secrecy if they believe it is in the public interest to release special operational information of CSEC. To date, no such matters have been reported to a Commissioner.

Reviewing CSEC activities

The purpose of my review mandate is:

- to ensure that activities conducted by CSEC under ministerial authorization are, in fact, those authorized by the Minister of National Defence;
- to ensure that CSEC complies with the law and, if I believe that it may not be complying, to report this to the Minister of National Defence and to the Attorney General of Canada;
- to ensure that CSEC does not direct its foreign signals intelligence and information technology (IT) security activities at Canadians; and
- to ensure that CSEC develops and effectively applies satisfactory measures to protect the privacy of Canadians in all the activities it undertakes.

Conducting investigations

My mandate includes undertaking any investigation I deem necessary in response to a written complaint — for example to determine whether CSEC has engaged, or is engaging, in unlawful activity or is not taking sufficient measures to protect the privacy of Canadians.

Once a written complaint is received, if I determine that it has merit and relates to my mandate, I have all the powers of a Commissioner under Part II of the *Inquiries Act* to access and review any information held by CSEC. I may also interview — under oath, if necessary — any CSEC employee to establish the facts concerning a complaint. I advise the complainant, the Minister of National Defence and the Chief of CSEC about the results of a formal complaint investigation. If I believe that CSEC may not have complied with the law, I would report this to the Minister and to the Attorney General of Canada.

Informing the Minister

Under my mandate, I also:

- report the results of my reviews, in classified reports, to the Minister of National Defence, who is accountable to Parliament for CSEC; and
- am required to submit an unclassified report to the Minister of National Defence on my activities each year, which the Minister must then table in Parliament. This is the 16th annual report.

My reviews focus on CSEC's compliance with its legal, ministerial and policy requirements. While it is my primary duty to report any non-compliance by CSEC, a necessary element of my mandate also includes informing CSEC of any activities that I believe might present, or have the potential to present, a risk of non-compliance, such as an unlawful interception of a private communication or other invasion of the privacy of a Canadian. If I am not satisfied that CSEC is responding to my concerns appropriately, I have the authority and the duty to report them to the Minister of National Defence. A number of my reports have included recommendations aimed at prevention. It is my goal to strengthen CSEC practices that contribute to compliance and incorporate measures that protect the privacy of Canadians. I believe it is ultimately more useful to prevent unlawful activity than to identify it after the fact.

Independence

While I submit my reports to the Minister responsible for CSEC, my office is independent and separate from the Department of National Defence. My review mandate is supported by the powers I have under the *Inquiries Act*. These powers ensure my access to all CSEC information and employees and include the power of subpoena. The independence of my mandate is further supported by the way my office is funded — it has been allocated its own appropriation from Parliament rather than receiving funding from the Department of National Defence.

Annex A contains the text of the relevant sections of the *National Defence Act* and the *Security of Information Act* relating to my role and mandate as CSE Commissioner (p. 41). **Annex B** describes the history of the Office of the CSE Commissioner (p. 45).

MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

When the *Anti-terrorism Act* came into effect on December 24, 2001, it added Part V.1 to the *National Defence Act*, and set out CSEC's three-part mandate:

> Part (a) authorizes CSEC to acquire and use foreign signals intelligence in accordance with the Government of Canada's intelligence priorities;
>
> Part (b) authorizes CSEC to help protect electronic information and information infrastructures of importance to the Government of Canada; and
>
> Part (c) authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies, including helping them obtain and understand communications collected under those agencies' own authorities.

Protection of Canadians

CSEC is prohibited by law from directing its foreign signals intelligence collection and IT security activities at Canadians — wherever they might be in the world — or at any person in Canada.

LIMITATIONS IMPOSED BY LAW ON CSEC

Parts (a) and (b) of CSEC's mandate

CSEC's activities related to the collection of foreign signals intelligence and to the protection of electronic information and information infrastructures of importance to the Government of Canada are subject to three legislative limitations aimed at protecting Canadians' privacy:

1. CSEC is prohibited from directing its foreign signals intelligence collection and IT security activities at Canadians, regardless of their location anywhere in the world, or at any person in Canada, regardless of their nationality;

2. In conducting these activities, CSEC may unintentionally intercept a communication that originates or terminates in Canada in which the originator has a reasonable expectation of privacy, which is a "private communication" as defined by the *Criminal Code*. CSEC *may* use and retain a private communication obtained this way but *only* if it is essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government of Canada computer systems or networks; and

3. To provide a formal framework for the unintentional interception of private communications while conducting foreign signals intelligence collection or IT security activities, the *National Defence Act* requires express authorization by the Minister of National Defence. These are known as ministerial authorizations. The Minister may authorize the activities once he or she is satisfied that specific conditions provided for in the Act have been met, which includes assurances of how such unintentional interceptions of private communications would be handled should they arise.

Private Communication: "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it" (section 183 of the *Criminal Code*).

Ministerial authorizations

When CSEC is conducting activities to acquire foreign signals intelligence, it cannot know beforehand with whom a targeted foreign entity outside Canada may communicate. Similarly, when CSEC is conducting activities to help protect Government of Canada computer systems, it cannot know beforehand who may communicate with or through that computer system. Given the complexity and interconnectedness of the global information infrastructure, it is unavoidable that CSEC will intercept a number of private communications. It is for this reason that CSEC requires a ministerial authorization for these activities — to shield itself from the *Criminal Code* in cases where it may unintentionally intercept a communication coming to or originating from Canada and where a person has an expectation of privacy. CSEC's ministerial authorizations relate to an "activity" or "class of activities" specified in the authorizations — that is, to a specific method of acquiring foreign signals intelligence or of protecting computer systems (the how); the authorizations do not relate to a specific individual or subject (the whom or the what).

Conditions for ministerial authorizations

To issue a ministerial authorization for foreign signals intelligence collection, the Minister must first be satisfied that:

- the interception will be directed at foreign entities located outside of Canada;
- the information could not be reasonably obtained by other means;
- the expected value of the interception would justify it; and
- satisfactory measures are in place to protect the privacy of Canadians and private communications will only be used or retained when essential to international affairs, defence or security.

To issue a ministerial authorization to protect the computer systems or networks of the Government of Canada, the Minister must be satisfied that:

- the interception is necessary;
- the information could not be reasonably obtained by other means;
- the consent of persons whose private communications may be intercepted could not reasonably be obtained;
- satisfactory measures are in place to ensure that only information essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and
- satisfactory measures are in place to protect the privacy of Canadians in the use and retention of that information.

Ministerial authorization: authorization provided in writing by the Minister of National Defence to CSEC so that CSEC is not in contravention of the *Criminal Code* if — in the conduct of foreign signals intelligence collection or IT security activities — it should unintentionally intercept a private communication. An authorization can be in effect for no longer than one year. In 2011–2012, there were six foreign signals intelligence collection and two IT security ministerial authorizations in effect.

Each year, I review all of CSEC's ministerial authorizations — which may be in effect for a period of no longer than one year — to ensure that the activities are authorized and that the above conditions for authorization are met. I report to the Minister of National Defence on my review.

Part (c) of CSEC's mandate

For CSEC to provide assistance to federal law enforcement and security agencies in fulfilling their mandated activities, the *National Defence Act* requires that those agencies first demonstrate that they have the legal authority — such as an authorization or a warrant — to conduct the activities. CSEC is then subject to the same laws and limitations that govern the agencies it is assisting rather than to the three legislative limitations listed above. In addition, ministerial authorizations do not apply to these activities.

MINISTERIAL REQUIREMENTS AND POLICIES TO PROTECT THE PRIVACY OF CANADIANS

CSEC's foreign signals intelligence and IT security activities are subject to measures, in addition to the limitations in the *National Defence Act*, that protect the privacy of Canadians in the use and retention of intercepted information.

Both CSEC's foreign signals intelligence and IT security program areas have dedicated sections responsible for day-to-day compliance and oversight. These two sections are important components of CSEC's management monitoring and accountability frameworks, and I examine their effectiveness as part of my reviews.

Handling of intercepted private communications

CSEC should use available means to reduce, to the extent possible, the unintentional interception of the private communications of Canadians. But what happens when CSEC's foreign signals intelligence and IT security activities result in unintentionally intercepted private

communications? If such unintentional interception does occur, these communications and information must be destroyed unless:

- they consist of foreign intelligence as defined in the *National Defence Act* and in accordance with the Government of Canada intelligence priorities;
- are essential to protect the lives or safety of individuals of any nationality;
- contain information on serious criminal activity relating to the security of Canada; or
- are essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

When ministerial authorizations expire, the Chief of CSEC must report to the Minister of National Defence information on the private communications unintentionally intercepted. These reports must state how many private communications were used or retained — on the basis, as required by law, that they are essential to international affairs, defence or security, or essential to identify, isolate or prevent harm to Government of Canada computer systems or networks. These reports must also include the number and value of any foreign intelligence reports produced from the intelligence derived from the private communications.

I examine the Chief's reports to the Minister, monitor the number of private communications unintentionally intercepted, and verify how CSEC treated and used these communications. I am able to review all of the private communications that CSEC uses and retains.

Directives and policies

Ministerial directives contain written direction to the Chief of CSEC on the Chief's duties and CSEC's activities. The June 2001 Ministerial Directive on *Communications Security Establishment Accountability Framework* sets out the accountability regime for CSEC, including a requirement for CSEC to report annually to the Minister of National Defence on CSEC's priorities and initiatives as

well as legal, policy and management issues of significance. The Chief's reports are one way I keep abreast of CSEC's activities. They also inform the development of my review work plan.

One ministerial directive in particular, the June 2001 Ministerial Directive on *Privacy of Canadians*, reinforces the requirements in the *National Defence Act* and ministerial authorizations. It requires CSEC to adopt measures to minimize the unintentional interception of private communications. It states that CSEC may retain and report information on or of Canadians, subject to specific criteria and appropriate measures in place for the handling, retention and destruction of this information. The treatment of this information must be consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*. Other ministerial directives provide guidance on specific CSEC activities.

CSEC's operational policy, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, applies to anyone conducting activities under CSEC authority, including CSEC employees and military personnel. It contains detailed measures for legal compliance and to safeguard the privacy of Canadians in the use and retention of intercepted information. Many other policies and procedures contain detailed requirements and provide instructions on specific CSEC activities and on measures to protect privacy. I review CSEC's activities to ensure compliance with ministerial directives and policies and procedures.

Information about Canadians: any personal information (as described in the *Privacy Act*) about a Canadian, including a Canadian corporation.

Canadian identity information

CSEC's reports may contain Canadian identity information, if that information is deemed essential to understand the reports. However, the reference to an identified Canadian must be suppressed and replaced by a generic reference such as "a named Canadian" person or company. When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting government department or agency has both the authority and the operational justification for obtaining the Canadian identity information. Only then may CSEC provide this information. Annually, I select and review a sample of these disclosures to verify that CSEC complies with the law and maintains measures to protect the privacy of Canadians.

International collaboration

CSEC and its closest international partners — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau — respect each other's laws by pledging not to target one another's citizens' communications. CSEC is prohibited from requesting an international partner to undertake activities that CSEC itself is legally prohibited from conducting. My reviews examine CSEC's cooperation with its allies to ensure compliance with the law.

CSEC training

CSEC's training program helps to ensure staff awareness of requirements and policies relating to lawfulness and the protection of the privacy of Canadians. Every new CSEC employee attends a foundational learning course, the curriculum of which includes information on legal and policy requirements and mandatory measures to protect privacy. For certain operational activities, CSEC's employees are required to participate in briefings on legal requirements prior to conducting the activities and at least yearly thereafter. During my reviews, I determine the extent to which this training is effective by questioning CSEC employees about their understanding of the requirements. **Annex C** contains text of relevant sections of the *National Defence Act* relating to the role and mandate of CSEC (p. 47).

COMMISSIONER'S OFFICE AND REVIEW PROCESS

I am supported in my work by a staff of eight, together with a number of subject-matter experts, under contract, as required. In 2011–2012, my office's expenditures were $1,942,429, which is within the budget provided by Parliament. An expansion to the physical space of my office is under way, which will allow me to hire additional employees.

Annex D provides the 2011–2012 Statement of Expenditures for the Office of the Communications Security Establishment Commissioner (p. 49).

Objective of review

The objective of my review is to enable me to provide to the Minister of National Defence, and indeed to all Canadians, assurance that CSEC is complying with the law and protecting the privacy of Canadians. If I were to find an instance where I believe CSEC may not have complied with the law, it would be my duty to inform the Minister of National Defence and the Attorney General of Canada.

Selection of activities for review

I use a risk-based and preventative approach to my reviews. I have a three-year work plan, which is updated twice per year. I draw on many sources to develop my work plan. My employees and I receive regular briefings from CSEC on new activities and on changes to existing activities of CSEC. I also go over the Chief of CSEC's annual report to the Minister of National Defence on CSEC's priorities and initiatives as well as legal, policy and management issues of significance. I then use a set of criteria to help select and prioritize CSEC activities based on where risk is greatest for potential non-compliance with the law including for risks to the privacy of Canadians.

Risk is assessed by considering, among other factors:

- the controls placed by CSEC on the activity to ensure compliance with legal, ministerial and policy requirements;
- whether the activity has the potential to involve private communications or information about Canadians;
- whether the activity is new, has changed significantly, or has had a lengthy period elapse since its last in-depth review;
- whether there have been significant changes to the authorities or technologies relating to the activity;
- whether Commissioners have made findings or recommendations relating to the activity that require follow-up; and
- issues arising in the public domain.

Review methodology and criteria

In conducting a review, my office examines CSEC's hard-copy and electronic information and records, as well as CSEC's policies and procedures and legal advice received from Justice Canada. My staff request briefings and demonstrations of specific activities, interview managers and employees and observe CSEC operators and analysts first hand to verify how they conduct their work. My staff test information obtained against the contents of systems and databases. The work of CSEC's internal auditors and evaluators may also inform reviews.

Each review includes an assessment of CSEC's activities against a standard set of criteria, described below, consisting of legal requirements, ministerial requirements, and policies and procedures. Each review may have additional criteria added, as appropriate.

> **Legal requirements**: I expect CSEC to conduct its activities in accordance with the *National Defence Act*, the *Privacy Act*, the *Criminal Code*, the *Canadian Charter of Rights and Freedoms* and any other relevant legislation, and in accordance with Justice Canada advice.

Ministerial requirements: I expect CSEC to conduct its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

Policies and procedures: I expect CSEC to have appropriate policies and procedures in place to guide its activities and to provide sufficient direction on legal and ministerial requirements including the protection of the privacy of Canadians. I expect employees to be knowledgeable about and comply with policies and procedures. I also expect CSEC to employ an effective management control framework for maintaining the integrity and lawful compliance of its activities. This includes appropriate accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

My review reports document CSEC's activities and practices and contain findings relating to the above-noted criteria. These reports may also disclose the nature and significance of deviations from the criteria. In some cases, I make recommendations to the Minister that are aimed at correcting discrepancies between CSEC's activities and the expectations established by the review criteria. I monitor how CSEC addresses recommendations and responds to negative findings. As well, I monitor areas for follow-up identified in past reviews.

The process of review is cumulative. Since my office was established in 1996, it has built up specific expertise in CSEC's unique mandate and activities. With each review my office adds to its knowledge of CSEC's activities and of how we can improve our own methodology. One such change implemented in recent years by my office was the introduction of horizontal reviews — that is, review of the processes by which CSEC selects foreign intelligence targets and uses, shares, reports, retains or disposes of intercepted information that are common to each of the activities or class of activities. This approach has provided for greater

depth of review. My office examines each of these common processes to determine whether CSEC complies with the law and the extent to which CSEC takes measures to protect the privacy of Canadians.

The Logic Model in **Annex E** provides a flow chart of our comprehensive review program (p. 50).

Horizontal reviews examine processes common to all CSEC foreign signals intelligence collection methods or IT security activities under ministerial authorization. For example, the processes by which CSEC:

- identifies, selects and directs its activities at entities of foreign intelligence interest;
- uses, shares, reports, retains or disposes of intercepted information; and
- takes measures to protect private communications intercepted unintentionally and Canadian identity information.

Recommendations

Since 1997, my predecessors and I have submitted to the Minister of National Defence 68 classified review reports. In total, the reports contained 133 recommendations. CSEC has accepted and implemented or is working to address 93 percent (124 out of 133) of these recommendations. Recommendations have contributed to CSEC suspending certain activities to re-examine how the activities are conducted and to restructure the processes and practices supporting the activities. This past year, CSEC completed work in response to one past recommendation and I am monitoring 15 recommendations that CSEC is working to address. I continue to await the Minister's response to one privacy-related recommendation I made in 2010–2011.

My website provides a complete list of the 68 classified review reports submitted to the Minister of National Defence (www.ocsec-bcest.gc.ca).

OVERVIEW OF 2011–2012 FINDINGS

During the 2011–2012 reporting year, I submitted seven reports to the Minister of National Defence on my review of CSEC activities.

These reviews were conducted under two areas of my mandate:

- ensuring CSEC activities are in compliance with the law — as set out in paragraph 273.63(2)(*a*) of the *National Defence Act*; and
- ensuring CSEC activities under a ministerial authorization are authorized — as set out in subsection 273.65(8) of the *National Defence Act*.

The results

Each year I provide a statement on my findings about the lawfulness of CSEC's activities in general. Overall, I am able to report that the activities of CSEC examined this year complied with the law. I made no recommendations this year. However, I made a number of suggestions to improve certain policies and practices the application of which I will be monitoring.

In some ways, it was a frustrating year due to delays in being able to proceed with some reviews. CSEC did not provide the same level of support to my office for these reviews, resulting in excessive delays. It has committed to correcting this situation. Ministerial direction requires the Chief of CSEC to support the Commissioner's reviews.

HIGHLIGHTS OF THE SEVEN REVIEWS SUBMITTED TO THE MINISTER IN 2011–2012

1. CSEC's retention and disposal of intercepted or copied communications

Background

The ever-increasing amount of electronic information being generated in our interconnected world has created challenges for CSEC in managing the retention (storage) and disposal (destruction) of the information it acquires. CSEC's foreign signals intelligence and IT security programs recently made significant technological changes impacting on their respective retention and disposal practices for acquired communications.

Paragraph 273.64(2)(*b*) of the *National Defence Act* requires CSEC to take measures to protect the privacy of Canadians. It includes the manner in which CSEC retains and disposes of communications that it intercepts in the conduct of its foreign signals intelligence collection and IT security activities. In this review, I paid particular attention to CSEC's retention and disposal of unintentionally intercepted private communications and Canadian identity information.

As a Government of Canada institution, CSEC also has a legal requirement to keep certain records. The *Access to Information Act* and the *Privacy Act* both recognize that citizens have the right, under specified conditions, to access government records. Federal institutions, such as CSEC, must also protect any personal information that they may collect or transmit. These legal requirements reinforce the obligation for CSEC to maintain a comprehensive and complete inventory and description of its information holdings. The unauthorized destruction of a record could result in an inability to document an activity, and consequently, an inability to demonstrate compliance.

My predecessors and I have always monitored CSEC's information management practices because the creation and retention of records is one of the main means by which CSEC can account for its activities and

provide assurance that its activities comply with legal, ministerial and policy requirements. My predecessors made a number of recommendations that resulted in significant developments in CSEC's information management practices and related systems to strengthen compliance.

Findings

I found that both CSEC's foreign signals intelligence collection and IT security programs have incorporated into the digital architectures of their respective programs a number of legal, ministerial and policy requirements relating to retention and disposal. I acquired detailed knowledge of and documented this policy-based and technology-assisted approach to CSEC information management practices. During this review, I found that CSEC built a number of automated compliance requirements into its systems to permit monitoring and auditing of its activities, as well as providing one level of proof of that compliance.

CSEC's policies and procedures for retention and disposal of acquired communications provide sufficient direction to CSEC employees respecting these activities and the protection of the privacy of Canadians. The retention and disposal periods set out in CSEC policies are reasonable. However, CSEC's inconsistent use of certain terminology in foreign signals intelligence and IT security policies is confusing and should be clarified. I will monitor CSEC efforts to clarify these policies.

I also found that CSEC had implemented recommendations made by my predecessors to establish records management authorities and retention and disposition schedules.

Conclusion

I concluded that CSEC conducted its retention and disposal activities during the period under review in accordance with legal and ministerial requirements and its policies and procedures.

2. CSEC's operations centre and particular foreign signals intelligence collection activities conducted in 2010

Background

CSEC's operations centre serves as the primary point through which CSEC interacts with Government of Canada clients, international partners and various internal CSEC sections during times of significantly elevated or unexpected activity. During such periods, the centre provides increased coordination. As part of its routine duties, the centre coordinates and produces a daily operational brief for the Chief of CSEC and provides other information to management, as required.

Findings

My review focused on an examination of the centre through an assessment of some of its activities conducted in 2010 under CSEC's mandates for foreign signals intelligence collection and assistance to federal law enforcement and security agencies. My highest priority was to assess the potential for risk posed to privacy in the conduct of these activities.

I also paid particular attention to CSEC's processing of requests from Government of Canada clients for releases of Canadian identity information suppressed in foreign signals intelligence reports produced by the centre. CSEC conducted these activities appropriately.

In novel or uncertain circumstances characteristic of an operations centre, I found that CSEC's use of temporary policy instruments to streamline approval processes in particular situations was appropriate. More broadly, CSEC managers and employees were aware of all relevant policies and procedures. CSEC managers routinely monitored their teams' activities to ensure compliance with both law and policy.

However, CSEC's operational instructions for some activities provided only limited direction specific to the nature of the operations centre. CSEC recognized this gap and is developing an operational instruction tailored to the centre's activities. I will monitor the implementation of this solution.

Conclusion

I concluded that CSEC conducted the examined activities in accordance with the law and ministerial requirements. A primary factor affecting my decision to review CSEC's operations centre was the potential for error in situations of increased pressure and time constraints. I found that, despite these circumstances in which the centre operated, the activities examined did not present any greater risk to compliance or to the privacy of Canadians than activities conducted by other sections of CSEC during routine business.

3. Update on an ongoing review of CSEC's foreign signals intelligence sharing with international partners

Background

It is common knowledge that Canada is a net importer of intelligence. CSEC's ability to fulfill its foreign signals intelligence collection and IT security mandates rests, in part, on building and maintaining productive relations with its foreign counterparts. CSEC's long-standing relationships with its closest allies — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau — continues to benefit CSEC, and, in turn, the Government of Canada. This cooperative alliance may be more valuable now than at any other time, in the context of increasingly complex technological challenges.

The global nature of terrorism requires security and intelligence agencies to cooperate and share information with one another. The Government of Canada's response to the Report of the Standing Committee on Public Safety and National Security *Review of the Findings and Recommendations Arising From the Iacobucci and O'Connor Inquiries*, recognized that:

> the exchange of information with foreign partners raises unique challenges — policy, legal and operational — that are examined

> on a case-by-case basis in the context of Canada's national security environment. The cumulative result of successive commissions of inquiry, reports and lessons learned has been the refinement of policies and practices surrounding the exchange of information between foreign partners and Canada's national security and intelligence and law enforcement communities. (p. 4)

The need for information sharing is vital. However, information must be exchanged in compliance with the laws of Canada and must include sufficient measures to protect the privacy of Canadians. Although these cooperative arrangements include a commitment by the partners to respect the privacy of each others' citizens, it is recognized each partner is an agency of a sovereign nation that may derogate from the agreements, if it is judged necessary for their respective national interests.

Past Commissioners have also examined specific aspects of CSEC's foreign signals intelligence collection cooperation and sharing with international partners. This year, as part of this focused review, I provided the Minister with an update on my ongoing review of these activities.

Findings

Thus far, I have found that CSEC does take measures to protect the privacy of Canadians in what it shares with its international partners. For example, CSEC suppresses Canadian identity information in what is shared with its international partners. In addition, open and ongoing communications among the partners helps to limit the potential to affect the privacy of a Canadian.

However, my review has also identified some important questions that I will continue to examine in the coming year, including: how does CSEC assure itself that its international partners follow the long-standing agreements and practices that provide a foundation for CSEC's foreign signals intelligence information sharing?

I will complete my review in 2012–2013.

4. Annual combined review of CSEC foreign signals intelligence ministerial authorizations

Background

Subsection 273.65(8) of the *National Defence Act* requires me to review CSEC activities carried out under ministerial authorizations "to ensure they are authorized and report annually to the Minister [of National Defence] on the review". An annual combined review of the foreign signals intelligence collection ministerial authorizations is one way that I fulfill this part of my mandate. This year, I examined the five foreign signals intelligence ministerial authorizations in effect in 2009–2010 relating to five activities or class of activities. The purpose of this annual combined review of the five foreign signals intelligence collection ministerial authorizations is to:

1. identify any significant changes to the ministerial authorization documents themselves or to CSEC's activities described in the authorizations;

2. assess the impact, if any, of these changes on the risk of non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and

3. examine a sample of my choosing of any resulting private communications unintentionally intercepted by CSEC during the conduct of the activities under the ministerial authorizations.

Findings

Within this approach, I assessed whether CSEC's foreign signals intelligence collection activities complied with the law and protected the privacy of Canadians. I found that the activities carried out by CSEC under these ministerial authorizations were authorized. I also reviewed a sample of private communications retained by CSEC but that were not used in CSEC reports. I found that CSEC retained only those private communications essential to international affairs, defence or security, as required by paragraph 273.65(2)(*d*) of the *National Defence Act*.

For each of the five foreign signals intelligence collection activities, I examined certain key information relating to interception and to the privacy of Canadians, to permit comparison of the activities and to identify any significant changes or trends over time.

The 2009–2010 foreign signals intelligence collection ministerial authorizations did not contain any significant changes from the previous year and CSEC did not make any significant changes to the technologies used for these activities. CSEC did, however, clarify and enhance associated operational policies, including direction relating to the protection of the privacy of Canadians.

In addition, the effective periods for the ministerial authorizations changed — starting and ending on different dates from previous years' authorizations. This affected my ability this year to examine year-to-year changes in certain metrics relating to interception and to the privacy of Canadians. In addition, certain information on intercepted communications involving CSEC's international partners was not readily available. I will examine this issue as part of my ongoing review of CSEC's foreign signals intelligence information-sharing activities with these partners.

I examined CSEC's activities in response to a 2009 recommendation that CSEC establish formal management processes for when CSEC considers undertaking certain proposed foreign signals intelligence collection activities and for the recording of the resulting decision. I found that CSEC addressed this recommendation in an amendment to an operational policy.

As of the end of the 2011–2012 reporting period, I am awaiting a response from the Minister of National Defence to a recommendation I made in last year's report that CSEC be required, in a ministerial authorization, to report to the Minister certain information relating to privacy. This requirement would support the Minister in his accountability for CSEC, including for the measures CSEC takes to protect the privacy of Canadians. The Minister had initially supported CSEC's rejection of this recommendation. However, I sent the Minister

further information and I understand that CSEC is now reviewing this matter. I remain of the view that CSEC should implement this recommendation.

CSEC implemented a compliance validation program for its foreign signals intelligence activities. Changes to associated operational policy are also under development to address a recommendation in my review last year on this subject, as well as in response to a related audit report by CSEC's internal auditors. Next year, I will begin a detailed review of CSEC's management control framework and how this program helps CSEC document and demonstrate compliance with legal and policy obligations.

Conclusion

Apart from the instance on maintaining a recommendation from 2010–2011, my review contained no recommendations.

5. Annual review of a sample of disclosures of Canadian identity information to Government of Canada clients for calendar year 2011

Background

My predecessor directed in 2010 that an annual review of a sample of disclosures of Canadian identity information to Government of Canada clients be conducted, to verify that CSEC continues to comply with the law and maintains measures to protect the privacy of Canadians.

Canadian identity information may be included in CSEC's foreign signals intelligence reports if it is required to understand or use foreign intelligence. However, any information that identifies a Canadian must be suppressed in the reports — that is, replaced by a generic reference such as "a named Canadian". When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC must verify that the requesting client has both the authority and operational justification for obtaining the Canadian identity information. Only then may CSEC provide that information.

Findings

I examined a sample representing approximately 20 percent of the total number of requests approved during the period under review. The sample included disclosures made to all of the Government of Canada departments and agencies that had requested Canadian identity information during the period under review. My officials examined: the requests documenting the clients' authority and justification for obtaining the Canadian identity information; associated CSEC foreign signals intelligence reports; and the actual disclosures of Canadian identity information.

I found that CSEC's disclosure of suppressed Canadian identity information to Government of Canada clients was conducted in compliance with the law. Operational policies and procedures are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians and CSEC employees were knowledgeable about, and acted in accordance with, the policies and procedures.

I also examined CSEC's progress since last year to address my 2010 recommendations relating to tools that could support the tracking of disclosures of Canadian identity information and improve the consistency and accuracy of related reporting. CSEC provided my officials with a demonstration of the capabilities of a new system for disclosures that has been introduced and will address the recommendations. I will continue to monitor the implementation of this system, and will ensure that it sufficiently incorporates safeguards to protect the privacy of Canadians.

Conclusion

My review did not result in any recommendations. However, my officials observed and communicated to CSEC that the section responsible for processing disclosure requests did not show its usual meticulousness during the period under review. Nevertheless, my officials found during their examination clear evidence that the activities were lawful and conducted in accordance with policies and procedures. While the gaps in CSEC's records did not lessen the protection of the

privacy of Canadians in respect of those disclosures, I alerted CSEC to these gaps for the purpose of eliminating them.

6. and 7. Annual review of incidents identified by CSEC in 2010 and annual review of incidents identified by CSEC in 2011 that affected or had the potential to affect the privacy of Canadians and the measures taken by CSEC to address them

Background

In 2007, the Chief of CSEC wrote to the Commissioner to inform him that CSEC had created a central file describing CSEC operational incidents that did or could impact the privacy of Canadians. The Chief indicated that the file would be made available to the Commissioner for review as a proactive means to demonstrate CSEC's commitment to protecting privacy, helping ensure transparency and enhancing public confidence in CSEC.

According to CSEC, it records in this central file any incidents that put at risk the privacy of a Canadian in a manner that runs counter to or is not provided for in its operational policies. CSEC policy requires CSEC foreign signals intelligence and IT security employees to report and document privacy incidents in order to demonstrate compliance with CSEC policies and legal requirements, and to prevent further incidents. Incidents could include the inadvertent inclusion of Canadian identity information in a report, or mistakenly sharing certain reports with the wrong recipient.

My reviews of CSEC activities include an examination of any privacy incidents relating to the subject under review. The objectives of such annual reviews are to: acquire knowledge of the incidents and of corrective actions; and inform development of my work plan, by determining if there are any systemic issues or issues about compliance with the law or the protection of the privacy of Canadians that should be

subject to follow-up review. The review of these privacy incidents identified by CSEC also assists me in evaluating CSEC's management control framework. My employees are vigilant during other reviews about identifying this type of error, so we can confirm whether CSEC also identified and addressed them.

2010 findings

In early 2011, I conducted an initial review of all of the 2010 privacy incidents in CSEC's central file, but did not complete the review in time to report last year. I examined all foreign signals intelligence and IT security privacy incidents and the subsequent actions taken by CSEC to correct the incidents, focusing on those incidents not examined in detail in my other reviews.

I was satisfied that CSEC took appropriate corrective actions in a timely manner in response to the privacy incidents it recorded during 2010. My review did not reveal any systemic deficiencies or issues that required follow-up review. I also noted that CSEC revised guidance about how to respond to certain privacy incidents.

2010 conclusion

My review of the privacy incidents in 2010 did not result in any recommendations. However, my officials identified and communicated to CSEC suggestions to make CSEC's central file complete and consistent, in particular concerning the assessment of potential consequences flowing from the privacy incidents, and verifying whether and when corrective actions had been taken.

2011 findings

In 2012, I examined all foreign signals intelligence and IT security privacy incidents recorded by CSEC in calendar year 2011, and the subsequent actions taken by CSEC to correct the incidents.

I was particularly interested in the remedial actions CSEC plans to take to address three particular privacy incidents. One involved CSEC issuing guidance to address a policy gap relating to CSEC exchanges of information containing Canadian identity information. This gap was

identified during one of my ongoing reviews. For two other privacy incidents relating to certain IT security activities, I am also pleased to note that CSEC will issue guidance for handling certain information and associated reporting. I will monitor CSEC's efforts to address these follow-on activities.

2011 conclusion

I am satisfied that CSEC took appropriate corrective actions in response to the privacy incidents it recorded in 2011. My review of the privacy incidents in 2011 did not reveal any systemic deficiencies or issues that require follow-up review. I did not make any recommendations.

I was generally satisfied that CSEC addressed the suggestions I made about it's central file in 2010 to make it complete and consistent. Most entries for 2011 contained sufficient information, including corrective and mitigation actions taken by CSEC or by its partner agencies.

COMPLAINTS ABOUT CSEC'S ACTIVITIES

In 2011–2012, I received no complaints about CSEC activities that warranted investigation. This is not surprising because CSEC directs its activities at foreign entities located outside Canada.

For details on the complaints process, visit the CSE Commissioner's website (www.ocsec-bccst.gc.ca).

DUTY UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information — such as certain information relating to CSEC's activities — on the grounds that it is in the public interest.

No such matters were reported to me in 2011–2012.

ACTIVITIES OF THE COMMISSIONER'S OFFICE

Review Agencies Forum

The Review Agencies Forum comprises officials from my office, the Security and Intelligence Review Committee (SIRC), the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints Against the Royal Canadian Mounted Police, and the Office of the Privacy Commissioner. The Forum contributes to the development of the review community through the exchange of expertise, research, developments in legislation and case law, and best practices relating to review. This year, a senior manager from the Security and Intelligence Secretariat of the Privy Council Office met with the Forum to discuss the government's national security priorities and developments as well as proposals to strengthen review agencies and address the findings of recent inquiries.

My office also delivered a second review workshop to provide formalized training to staff from Forum organizations that are relatively new to the function of review.

Code of Values, Ethics and Conduct

I approved a Code of Values, Ethics and Conduct that applies to all individuals employed by my office. The Code contains specific responsibilities and expected behaviours of employees relating to the conduct of their work and reviews of CSEC. This Code fulfills the requirement of section 5 of the *Public Servants Disclosure Protection Act*. I am confident that commitment to these values and observance of the Code's behaviours will strengthen the ethical culture of the Commissioner's office and contribute to its integrity.

Other activities

In September, my office's Executive Director met with a Brazilian Federal Prosecutor who was a visiting academic at the Canadian Centre for Intelligence and Security Studies of Carleton University. This meeting informed the prosecutor's work on accountability and review mechanisms for Brazilian intelligence activities.

In October, my office's Executive Director, Director of Operations and legal counsel joined me at the Canadian Institute for the Administration of Justice's conference, *Terrorism, Law and Democracy: 10 years after 9/11*. Leading experts on national security law, privacy and related topics explored how changes to Canadian law to combat terrorism have affected fundamental rights and values of procedural justice in the last decade. Together with the former Independent Reviewer of Terrorism Legislation in the United Kingdom and the former Chair of SIRC, I participated in a panel on procedure and accountability in anti-terrorism matters. We discussed the role and importance of independent review of security and intelligence agencies in the Canadian and international contexts.

Also in October, officials from my office participated in a conference on the integration of privacy rights into security technologies, *Vers une intégration du droit à la vie privée et des technologies de sécurité*. The conference was organized by the *Centre de recherche en droit public* of the University of Montréal. My Executive Director participated in a panel and provided his perspectives on distinctions between national security and public safety and the integration of technology and privacy protection in national security. This conference also afforded my employees an opportunity to meet with Canadian and international civil servants, academics and students interested in issues of privacy, national security and public safety.

In November, my employees and I attended the annual international conference of the Canadian Association for Security and Intelligence Studies (CASIS) in Ottawa. For the past 10 years, my office has supported CASIS conferences and seminars offered to members and students interested in broadening understanding of the issues affecting security and intelligence. Under this year's theme, *New Frontiers in Security and Intelligence*, the conference explored new developments in this field.

The activities of CSIS are subject to review by SIRC. Those of CSEC are subject to review by me. SIRC and my own office are two separate, distinct and autonomous entities. SIRC may not investigate CSEC activities. My office may not investigate CSIS activities. It follows that when CSEC is acting at the request of CSIS, my powers of review begin only at the moment the request is made and are confined to the activities of CSEC — from the time the request is made, to the delivery of any information to CSIS. This year, I initiated discussions with the Chair and members of SIRC, and my Executive Director forwarded to SIRC a discussion paper on proposals for varying levels of cooperation in the conduct of reviews of activities involving both CSEC and CSIS. As I noted in my introduction, there is opportunity, under existing authorities, for greater collaboration between SIRC and my office, to enhance the effectiveness of review, in the spirit of the recommendations of the commission of inquiry led by the Honourable Justice Dennis O'Connor. In the coming year, I will pursue discussion of proposals to enhance collaboration of reviews of joint CSEC-CSIS activities.

CSEC is a highly technical organization, and my office is expected to keep pace with the rapid technological changes affecting CSEC's activities. For this reason, CSEC includes my employees in CSEC training, including introductory courses CSEC provides to new employees and training for the use of specific systems and databases.

WORK PLAN — REVIEWS UNDER WAY AND PLANNED

The results of several reviews currently underway are expected to be reported to the Minister of National Defence in the coming year and will be included in my 2012–2013 annual report.

The subjects of these reviews include: CSEC's foreign signals intelligence sharing with international partners; assistance to CSIS under CSEC's mandate to provide support to federal law enforcement and security agencies and sections 12 and 21 of the *CSIS Act*; and CSEC IT security activities conducted in support of Government of Canada departments' authorities under the *Criminal Code* and the *Financial Administration Act*.

Other reviews planned for 2012–2013, which may carry over to the next year, include reviews of: CSEC's Office of Counter-Terrorism and its activities and interactions with CSIS; particular signals intelligence collection activities conducted under ministerial authorizations; IT security activities conducted under ministerial authorizations; and CSEC's management control framework and compliance monitoring activities.

In addition, I will continue the annual reviews of foreign signals intelligence ministerial authorizations, CSEC disclosures of Canadian identity information to government clients, and privacy incidents identified by CSEC and the measures subsequently taken by CSEC to address them.

THE UPCOMING YEAR

The coming year promises to be eventful.

In May 2012, Canada hosts the 8th International Intelligence Review Agencies Conference in Ottawa. This is the second time that Canada is hosting this biennial conference, created in 1997. This year, it will bring together representatives of review bodies from 10 countries.

This Conference constitutes a unique opportunity for all of us to each share our experiences with the others and to gain from drawing comparisons. When it comes to review, there is no standard structure. Some countries stress the role of Parliamentarians, others that of independent review bodies headed by appointed officials. Canada will use this opportunity to report on changes since we last hosted the Conference in 1999. This retrospective over the past thirteen years should give us the necessary perspective to better assess today's reality and better predict tomorrow's.

This opportunity for perspective comes at the right time. The studies undertaken in Canada in recent years, particularly in the wake of the recommendations of Commissioners O'Connor, Iacobucci and Major on the possible reorganization of the intelligence and security review community, should bear fruit before long. Will some organizations be

shut down? — or merged? — or a new one created? — or a super-organization set up? Will there be a role for Parliamentarians and, if so, what kind? These are all questions that will give rise to a promising debate to which I look forward to contributing.

I must raise once again the matter of clarifying certain provisions of the *National Defence Act*, something my predecessors and I have proposed repeatedly. I concede that this is a matter of opportunity and political context. But I confess to being deeply disappointed at the time that has passed without addressing the ambiguities in the Act which, to my mind, should raise no controversy.

Finally, the title I have been given, Commissioner of the Communications Security Establishment, gives the impression that I am part of CSEC, whereas, on the contrary and for the reasons that led to my position being created in the first place, I am entirely independent. I have asked that this unfortunate designation be corrected.

ANNEX A: EXCERPTS FROM THE *NATIONAL DEFENCE ACT AND THE SECURITY OF INFORMATION ACT* RELATED TO THE MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

***National Defence Act* – Part V.1**

Appointment of Commissioner

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

Duties

(2) The duties of the Commissioner are:

(*a*) to review the activities of the Establishment to ensure that they are in compliance with the law;

(*b*) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(*c*) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

Annual report

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

Powers of investigation

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the Inquiries Act.

Employment of legal counsel, advisors, etc.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

Directions

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

Transitional

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

Review of authorizations

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

Public interest defence

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

Prior disclosure to authorities necessary

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX B: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the late Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., former Chief Justice of Canada, for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006, a position he held until his death in July 2009. The Honourable Peter deC. Cory, C.C., C.D., also a former Justice of the Supreme Court of Canada, served as Commissioner from December 14, 2009, to March 31, 2010. On June 18, 2010, the Honourable Robert Décary, Q.C., a former Justice of the Federal Court of Appeal, was appointed Commissioner.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

The omnibus *Anti-terrorism Act*, which came into force on December 24, 2001, introduced amendments to the *National Defence Act* by adding Part V.1 and creating legislative frameworks for both the Commissioner's office and CSEC. It gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

While the Commissioner continues to provide the Minister of National Defence with his reports, the Commissioner's office is separate from, and not part of, the Department of National Defence.

ANNEX C: EXCERPTS FROM THE *NATIONAL DEFENCE ACT* RELATED TO THE MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency, providing the Government of Canada with two key services: foreign signals intelligence, and information technology security. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign signals intelligence products and services support government decision-making in the fields of national security, national defence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable government departments and agencies to secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC's three-part mandate is set out in subsection 273.64(1) of the *National Defence Act*:

> (*a*) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (*b*) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (*c*) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

CSEC's website is: www.cse-cst.gc.ca.

ANNEX D: 2011-2012 STATEMENT OF EXPENDITURES

Standard Object Summary ($)

Salaries and Benefits		1,022,064
Transportation and Telecommunications		15,998
Information		11,652
Professional and Special Services		386,906
Rentals		168,110
Repairs and Maintenance		235
Material and Supplies		12,164
Machinery and Equipment		12,070
Assets		
Communications Equipment	29,759	
Office Equipment and Furniture	50,031	
Informatics Equipment	38,700	
Leasehold Improvements in Progress	194,740	
		313,230
Total		**1,942,429**

ANNEX E: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL